WE CLAIM

1. A computer program product for operating a computer to review files for potential malware, comprising:

logging code operable to maintain a statistical log having an entry for each file sent to the computer for review, each entry being arranged to store a count value indicating the number of times that the file has been sent to the computer for review and a value of one or more predetermined attributes relating to the file;

weighting table code operable to maintain a weighting table identifying, for each value of said one or more predetermined attributes, a weighting indicating the likelihood that a file having that value of said one or more predetermined attributes will be malware;

statistical log interface code operable, upon receipt of a file, to determine with reference to the statistical log the count value relating to that file;

action determination code operable, if the count value determined by the statistical log interface code exceeds a predetermined threshold, to reference the weighting table to determine the weighting to be associated with the file, based on the value of said one or more predetermined attributes associated with that file in the statistical log; and

action performing code operable to perform predetermined actions in relation to the file dependent on the weighting determined by said action determination code.

2. A computer program product as claimed in Claim 1, wherein said one or more predetermined attributes comprise an indication of the file type of the file.

3. A computer program product as claimed in Claim 1, wherein if the weighting indicates that the file is probably malware, said action performing code is operable to perform the steps of:

(i) encrypting the file such that only an administrator can decrypt that file; and

(ii) generating for access by an administrator a notification identifying that the file has been encrypted.

4. A computer program product as claimed in Claim 3, wherein the action performing code is further operable to associate a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted.

5. A computer program product as claimed in Claim 1, wherein if the weighting indicates that the file is possibly malware, said action performing code is operable to perform the steps of:

(i) encrypting the file such that only an administrator or the originator of the file can decrypt that file; and

(ii) generating for access by an administrator a notification identifying that the file has been encrypted.

6. A computer program product as claimed in Claim 5, wherein the action performing code is further operable to associate a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted.

7. A computer program product as claimed in Claim 1, wherein if the weighting indicates that the file is to be treated with caution, said action performing code is operable to perform the steps of:

(i) associating a warning message with the file for reference by a person receiving that file; and

(ii) generating for access by an administrator a notification identifying the file.

8. A computer program product as claimed in Claim 1, wherein if the weighting indicates that the file is safe, said action performing code is operable to generate for access by an administrator a notification identifying the file.

9. A computer program product as claimed in Claim 1, wherein if it is determined that a file sent to the computer is not currently entered in the statistical log, the logging code is further operable to create an entry in the statistical log for the file, in which the

value of said one or more predetermined attributes relating to the file are stored, and in which the count value is initialised.

10. A computer program product as claimed in Claim 1, wherein upon receipt of a file, the statistical log interface code is operable to cause the count value within the relevant entry of the statistical log to be incremented to account for the current occurrence of the file.

11. A computer program product as claimed in Claim 1, wherein the computer is arranged to review files included in e-mail communications, and each entry in the statistical log is further arranged to identify, for each sender of that file, the number of times that that sender has sent the file in addition to the count value indicating the total number of times that the file has been sent.

12. A computer program product as claimed in Claim 11, wherein upon receipt of a file, the statistical log interface code is operable to cause the count value within the relevant entry of the statistical log to be incremented to account for the current occurrence of the file, and the number by which the count value is incremented is dependent on the number of times that the sender of the current occurrence of the file has previously sent that file.

13. A computer program product as claimed in Claim 1, wherein if said action performing code is arranged, dependent on the weighting, to encrypt the file, the computer program product further comprises:

automated decryption code operable, if the file is subsequently determined to be safe, to perform the steps of:

(i) locating all encrypted occurrences of that file on a file system; and

(ii) decrypting each said occurrence.

14. A method of operating a computer to review files for potential malware, comprising the steps of:

(a) maintaining a statistical log having an entry for each file sent to the computer for review, each entry being arranged to store a count value indicating the number of times that the file has been sent to the computer for review and a value of one or more predetermined attributes relating to the file;

(b) maintaining a weighting table identifying, for each value of said one or more predetermined attributes, a weighting indicating the likelihood that a file having that value of said one or more predetermined attributes will be malware;

(c) upon receipt of a file, determining with reference to the statistical log the count value relating to that file;

(d) if the count value determined at said step (c) exceeds a predetermined threshold, referencing the weighting table to determine the weighting to be associated with the file, based on the value of said one or more predetermined attributes associated with that file in the statistical log; and

(e) performing predetermined actions in relation to the file dependent on the weighting determined at said step (d).

15. A method as claimed in Claim 14, wherein said one or more predetermined attributes comprise an indication of the file type of the file.

16. A method as claimed in Claim 14, wherein if the weighting indicates that the file is probably malware, said step (e) comprises the steps of:

(i) encrypting the file such that only an administrator can decrypt that file; and

(ii) generating for access by an administrator a notification identifying that the file has been encrypted.

17. A method as claimed in Claim 16, further comprising the step of associating a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted.

18. A method as claimed in Claim 14, wherein if the weighting indicates that the file is possibly malware, said step (e) comprises the steps of:

(i) encrypting the file such that only an administrator or the originator of the file can decrypt that file; and

(ii) generating for access by an administrator a notification identifying that the file has been encrypted.

19. A method as claimed in Claim 18, further comprising the step of associating a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted.

20. A method as claimed in Claim 14, wherein if the weighting indicates that the file is to be treated with caution, said step (e) comprises the steps of:

(i) associating a warning message with the file for reference by a person receiving that file; and

(ii) generating for access by an administrator a notification identifying the file.

21. A method as claimed in Claim 14, wherein if the weighting indicates that the file is safe, said step (e) comprises the step of generating for access by an administrator a notification identifying the file.

22. A method as claimed in Claim 14, wherein if at said step (c) it is determined that the file is not currently entered in the statistical log, the method further comprises the step of creating an entry in the statistical log for the file, in which the value of said one or more predetermined attributes relating to the file are stored, and in which the count value is initialised.

23. A method as claimed in Claim 14, wherein said step (c) includes the step of incrementing within the statistical log the count value to account for the current occurrence of the file.

24. A method as claimed in Claim 14, wherein the computer is arranged to review files included in e-mail communications, and each entry in the statistical log is further

arranged to identify, for each sender of that file, the number of times that that sender has sent the file in addition to the count value indicating the total number of times that the file has been sent.

25. A method as claimed in Claim 24, wherein said step (c) includes the step of incrementing within the statistical log the count value to account for the current occurrence of the file, and the number by which the count value is incremented is dependent on the number of times that the sender of the current occurrence of the file has previously sent that file.

26. A method as claimed in Claim 14, wherein if at said step (e), the file is encrypted, the method further comprises, if the file is subsequently determined to be safe, the automated steps of:

locating all encrypted occurrences of that file on a file system; and

decrypting each said occurrence.

27. A data processing apparatus for reviewing files for potential malware, comprising:

logging logic operable to maintain a statistical log having an entry for each file sent to the computer for review, each entry being arranged to store a count value indicating the number of times that the file has been sent to the computer for review and a value of one or more predetermined attributes relating to the file;

weighting table logic operable to maintain a weighting table identifying, for each value of said one or more predetermined attributes, a weighting indicating the likelihood that a file having that value of said one or more predetermined attributes will be malware;

statistical log interface logic operable, upon receipt of a file, to determine with reference to the statistical log the count value relating to that file;

action determination logic operable, if the count value determined by the statistical log interface logic exceeds a predetermined threshold, to reference the weighting table to determine the weighting to be associated with the file, based on the

value of said one or more predetermined attributes associated with that file in the statistical log; and

action performing logic operable to perform predetermined actions in relation to the file dependent on the weighting determined by said action determination logic.

28. A data processing apparatus as claimed in Claim 27, wherein said one or more predetermined attributes comprise an indication of the file type of the file.

29. A data processing apparatus as claimed in Claim 27, wherein if the weighting indicates that the file is probably malware, said action performing logic is operable to perform the steps of:

(i) encrypting the file such that only an administrator can decrypt that file; and

(ii) generating for access by an administrator a notification identifying that the file has been encrypted.

30. A data processing apparatus as claimed in Claim 29, wherein the action performing logic is further operable to associate a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted.

31. A data processing apparatus as claimed in Claim 27, wherein if the weighting indicates that the file is possibly malware, said action performing logic is operable to perform the steps of:

(i) encrypting the file such that only an administrator or the originator of the file can decrypt that file; and

(ii) generating for access by an administrator a notification identifying that the file has been encrypted.

32. A data processing apparatus as claimed in Claim 31, wherein the action performing logic is further operable to associate a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted.

33. A data processing apparatus as claimed in Claim 27, wherein if the weighting indicates that the file is to be treated with caution, said action performing logic is operable to perform the steps of:

(i) associating a warning message with the file for reference by a person receiving that file; and

(ii) generating for access by an administrator a notification identifying the file.

34. A data processing apparatus as claimed in Claim 27, wherein if the weighting indicates that the file is safe, said action performing logic is operable to generate for access by an administrator a notification identifying the file.

35. A data processing apparatus as claimed in Claim 27, wherein if it is determined that a file sent to the computer is not currently entered in the statistical log, the logging logic is further operable to create an entry in the statistical log for the file, in which the value of said one or more predetermined attributes relating to the file are stored, and in which the count value is initialised.

36. A data processing apparatus as claimed in Claim 27, wherein upon receipt of a file, the statistical log interface logic is operable to cause the count value within the relevant entry of the statistical log to be incremented to account for the current occurrence of the file.

37. A data processing apparatus as claimed in Claim 27, wherein the computer is arranged to review files included in e-mail communications, and each entry in the statistical log is further arranged to identify, for each sender of that file, the number of times that that sender has sent the file in addition to the count value indicating the total number of times that the file has been sent.

38. A data processing apparatus as claimed in Claim 37, wherein upon receipt of a file, the statistical log interface logic is operable to cause the count value within the relevant entry of the statistical log to be incremented to account for the current

occurrence of the file, and the number by which the count value is incremented is dependent on the number of times that the sender of the current occurrence of the file has previously sent that file.

39. A data processing apparatus as claimed in Claim 27, wherein if said action performing logic is arranged, dependent on the weighting, to encrypt the file, the data processing apparatus further comprises:

automated decryption logic operable, if the file is subsequently determined to be safe, to perform the steps of:

(i) locating all encrypted occurrences of that file on a file system; and

(ii) decrypting each said occurrence.